Published and Copyright (c) 1999 - 2015
All Rights Reserved

Atari Online News, Etc.
A-ONE Online Magazine
Dana P. Jacobson, Publisher/Managing Editor
Joseph Mirando, Managing Editor
Rob Mahlert, Associate Editor

Atari Online News, Etc. Staff

Dana P. Jacobson -- Editor
Joe Mirando -- "People Are Talking"
Michael Burkley -- "Unabashed Atariophile"
Albert Dayes -- "CC: Classic Chips"
Rob Mahlert -- Web site
Thomas J. Andrews -- "Keeper of the Flame"

With Contributions by:

Fred Horvat

To subscribe to A-ONE, change e-mail addresses, or unsubscribe, log on to our website at: www.atarinews.org and click on "Subscriptions".
OR subscribe to A-ONE by sending a message to: dpj@atarinews.org and your address will be added to the distribution list.
To unsubscribe from A-ONE, send the following: Unsubscribe A-ONE
Please make sure that you include the same address that you used to subscribe from.

To download A-ONE, set your browser bookmarks to one of the following sites:

http://people.delphiforums.com/dpj/a-one.htm
Now available:
http://www.atarinews.org

Visit the Atari Advantage Forum on Delphi!
http://forums.delphiforums.com/atari/

=~=~=~=

~ Beebone Botnet Downed! ~ People Are Talking! ~ New OS X Released!
~ China Internet Cannon! ~ Sony May Owe You Money! ~ Edgar Vigdal, R.I.P.

~ Blizzard Blocks Crimea ~ Facebook Tracks Non-use ~ Facebook Still Cool!
~ Facebook Denies Report ~ Google vs Ad-injectors! ~ .sucks Controversy!

-* "Atari: Game Over" on Netflix *-
-* Net Neutrality Complaints Readying! *-
-* Obama Signs Off To Sanction Foreign Hackers *-

=~=~=~=

->From the Editor's Keyboard "Saying it like it is!"
""""""""""""""""""""""""""""

We're in the second week of April already, and we're still being hit with winter weather and bone-chilling temperatures! However, that could change starting this weekend. We're all hoping that Spring will finally arrive! Only a few piles of snow remain in my yard, leaving a glaring display of "debris" strewn throughout my yard from this year's harsh winter. It's going to take some time to get everything cleaned up this year!

Lots of interesting news this week - hoping you'll enjoy the offerings. I've said it in the past, but I want to repeat it again while it's on my mind: I want to publicly thank one of our loyal readers, Fred Horvat, for being such a consistent contributor to A-ONE. A week rarely goes by without my receiving numerous e-mails from Fred with either articles or links to articles online that he feels might be of interest to our readers. Many weeks, if it weren't for Fred's contributions, the mag would consist of much smaller offerings! Thanks Fred!

Until next time...

=~=~=~=

->In This Week's Gaming Section - Blizzard Blocks Games in Crimea!
""""""""""""""""""""""""""""""" Buy A Vita, Sony May Owe You!
"Atari: Game Over" on Netflix!
And much more!

=~=~=~=

->A-ONE's Game Console Industry News - The Latest Gaming News!
""""""""""""""""""""""""""""""""""""

Blizzard Blocks 'World of Warcraft' and 'Diablo 3' in Crimea

Players in Crimea can no longer access Battle.net, the service that houses Blizzard games World of Warcraft, Diablo 3, Hearthstone and others, The Moscow Times reports. Blizzard blocked its games in response to US sanctions against Crimea -- Google, Apple, PayPal and Valve have also suspended service to the region, the site says. The Moscow Times pulled its Blizzard report from Russian site Geektimes.ru, which published an email sent to Crimean Battle.net users. "In accordance with current trade regulations relating to the region of Crimea, we are legally required to suspend access to your Battle.net account," a translation reads.

President Barack Obama in December signed an executive order prohibiting the export of goods, technology or services to Crimea, matching similar sanctions from Europe. Crimea is in a high-stakes limbo at the moment, pulled between Russian and Ukranian rule. Russia seized and annexed the region in early 2014, though most nations, including the US, don't recognize this claim and instead view Crimea as an autonomous republic of Ukraine. The battle over Crimea has dramatically heightened tensions between the Western world and Russia. Blizzard's block is the latest move in a larger international push to remove Russian forces from the peninsula.

Did You Buy a PlayStation Vita Before June 2012? Sony Owes You Money

The lawyers behind a class action lawsuit against Sony over deceptive advertising for the PlayStation Vita have launched a website for potential claimants to sign up in order to collect their award. Anyone who purchased a PlayStation Vita before June 1, 2012 and who has not returned it for a full refund is entitled to part of the FTC-mandated award. If you qualify, head over to VitaClaims.com to fill out the form.

Eligible claimants must fill out the form by June 29, 2015 in order to collect. They will be asked to provide their Vita s serial number, which will be used to verify its date of purchase. Then they will have a choice of how they wish to be compensated: a $25 check, $25 in credit for the PlayStation Store, or one of three bundles of games for the PS3 and Vita, with combined retail values (helpfully included) of over $50:

Action/Adventure: God of War Collection, Beyond: Two Souls, Twisted Metal, Unity 13 ($92.95)
Family Friendly: LittleBigPlanet 2, Puppeteer, Uncharted: Golden Abyss, ModNation Racers: Road Trip ($100.46)
Variety Pack: God of War Collection, LittleBigPlanet 2, ModNation Racers: Road Trip, Unit 13 ($66.46)

The Federal Trade Commission filed a complaint against Sony in 2014 over deceptive claims concerning the PlayStation Vita s game-changing capabilities, made in advertisements leading up to the handheld s launch in 2012. The pre-launch advertising exaggerated the system s remote play and cross-save integration with the PlayStation 3, implying that these features would be generally available. In reality, this feature was only available for a few PS3 games, and the pause-and-save capability described in the ads varied significantly from game to game, according to the FTC complaint.

The commercial shows someone pausing his game of MLB 12: The Show on PS3 and immediately picking it up on his Vita while heading to work. In reality, the only way to transfer a save over was after completing all nine innings of a game. Sony s advertisements also failed to make clear that in order to use the feature, the player needed to purchase the game separately on each respective platform. Cross-Buy has subsequently become a more common feature of games released on multiple Sony platforms, but it was not standard at the time.

Nintendo Shows Earthbound Reward As Sold Out For Club Nintendo Members

This is a good time to remind our readers that Club Nintendo is ending. You can no longer earn coins for registering products, and those you already have are going to expire in a few months, but one of the offerings seems to be out of stock, at least temporarily.

Kotaku spotted that Earthbound for Wii U, one of the many digital rewards on offer, is showing up as sold out. We checked a random sample of 10 other titles (leaning toward those that might be considered more popular, like Star Fox 64, Kid Icarus Uprising, Super Metroid, and Donkey Kong Country Returns 3D), and all were still available.

We ve reached out to Nintendo for clarification on whether this is a glitch or if stock has really been depleted. We ll update should we receive a response.

The way the system works is that when you pick an item, a code is shown immediately (and also delivered via email). If Earthbound has proven to be immensely popular (as we would expect it to be), it could simply be a matter that more codes will be generated to populate the database. The same thing has happened infrequently on Steam during its big sales.

There s no need to panic quite yet. However, if it does turn out that the digital rewards are limited in number, we expect there will be another run on the system (which will likely bring it to its knees again). Stay tuned for more information.

=~=~=~=

->A-ONE Gaming Online - Online Users Growl & Purr!

Documentary of Atari Dig in the New Mexico Desert on Netflix

A documentary on Atari’s decline and a decades-old urban legend on the secret dumping of the "E.T." game in the New Mexico desert is airing on Netflix.

"Atari: Game Over" was released on the streaming service late Wednesday and details the demise of gaming giant Atari. The documentary also

investigates claims that Atari hid its biggest flop, 1982's "E.T.," by burying the cartridges in an Alamogordo, New Mexico, dump.

The "E.T." game had the reputation of being the worst game ever made and contributed to the demise of the company.

Around 300 and 400 games uncovered in the New Mexico landfill last year were later sold on eBay.

Edgar Vigdal Passes Away

From the EMV Software site:

Some very sad and very serious news for everyone following the development of Warblade Mk II and Deluxe Galaga Reborn. Unfortunately Edgar Vigdal passed away on the evening of the 1st April 2015 of cancer. I believe the death of his father and the toll that brought on him along with his lifelong illnesses had worn him down. We are all shocked and saddened by this news and my deepest warmest thoughts are with his family and friends. I will miss Edgar very much, he has been a big part of my life for many many years now through our long chats and late nights on Skype.

RIP my great friend. Keep on coding...

Simon Quincey.

=~=~=~=

A-ONE's Headline News
The Latest in Computer Technology News
Compiled by: Dana P. Jacobson

Backbone Providers Readying Net Neutrality Complaints

Indications are that the dispute over the Federal Communications Commission's (FCC) new Net neutrality rules might just be settled in court. Cogent Communications, which controls parts of the Internet backbone, is preparing to file complaints with the FCC, charging Internet service providers Comcast, Time Warner Cable, AT&T, Verizon, and CenturyLink with improperly degrading Internet traffic.

Cogent CEO Dave Schaeffer told the National Journal that if those companies continue to refuse to provide their customers "with access to the entire Internet on an unfettered basis . . . we would have no choice but to file a complaint with the FCC under the Open Internet Order."

Internet backbone provider Level 3 Communications said in an e-mail statement that it is also currently evaluating its options.

While the Net neutrality rules mandate that Internet service providers

should not block or degrade traffic once it’s on their networks, the complaints from Cogent and Level 3 would focus on how so-called last mile providers load traffic onto their networks. However, the dispute might not interest consumers initially, Hunter Newby, CEO of New York-based collocation and interconnection provider Allied Fiber, told us.

"People just want better, faster, cheaper," he said. "The FCC is casting a vision of protecting people’s rights. This comes in the form of making a rule that keeps Internet access providers from blocking, or degrading any content on their network."

Backbone providers transport data from Web sites to the Internet service providers, which then deliver the Internet content to people’s homes. Most network operators exchange traffic without charging any fees under the idea that both benefit by freely exchanging traffic back and forth.

The expansion of online video streaming services such as Netflix has upset the equation. Netflix alone now accounts for more than one-third of all U.S. Internet traffic during peak hours.

The companies will be able to file their complaints once the rules go into effect, which happens 60 days after they are published in the Federal Register. The rules are set to be formally published on Monday.

The backbone providers have been trying to push huge amounts of traffic through connections that were intended for much smaller exchanges. In many cases, that congestion resulted in grainy and choppy videos for customers. The Internet service providers have been demanding payments to build better connections for the traffic.

"The semantics of when content actually reaches an access provider’s network is where the entire Open Internet Rule falls apart," said Newby. "If the access providers can claim that some kind of content did not yet reach their access network, they will be able to block and degrade it without penalty."

Obama Signs Executive Order To Sanction Foreign Hackers

President Obama just used perhaps the most effective tool in his arsenal to strike against the threat of foreign cyberattacks - that’s right, his pen.

Obama signed a new executive order on Wednesday (1 April 2015) authorizing financial sanctions against foreign hackers, and companies that knowingly benefit from cyberattacks against US interests.

In a statement published on Medium, the US president pointed a finger directly at China, Russia, North Korea and Iran as examples of the threat.

Law enforcement, international cooperation and diplomacy aren’t enough to counter foreign nation states and individuals that have targeted the US military, infrastructure, and private companies, Obama said.

An executive order relies on the president’s authority under existing laws to direct the activities of government agencies - in this case, the US Department of the Treasury.

Reflecting just how frequent and severe cyberattacks have become from state-sponsored actors and cybercriminal organizations, the US has grown increasingly bold in calling out other nations for conducting espionage against US companies and government institutions.

Obama mentioned the breach of Sony Pictures in 2014 that the US claims was directed by North Korea in retaliation for the release of The Interview, a satirical movie mocking the country's leader, Kim Jong Un.

Although the Obama Administration levied sanctions against North Korean individuals in retaliation for the attack on Sony, the White House said those sanctions were authorized specifically to target the North Korean regime.

The new executive order is much more far-reaching, allowing the US to freeze the financial assets of any individual responsible or complicit in cyberattacks that pose a significant threat to US national security, foreign policy and economic stability.

According to a White House statement:

This Executive Order authorizes the Secretary of the Treasury, in consultation with the Attorney General and the Secretary of State, to impose sanctions on those individuals and entities that he determines to be responsible for or complicit in malicious cyber-enabled activities that are reasonably likely to result in, or have materially contributed to, a significant threat to the national security, foreign policy, economic health, or financial stability of the United States.

The order also authorizes sanctions against "a corporation that knowingly profits from stolen trade secrets."

The US Department of Justice last year took the unprecedented step of indicting five Chinese military officers on charges alleging they were responsible for espionage attacks against US steel and energy companies.

But those indictments will likely never result in the Chinese officers being extradited to the US to face prosecution.

In recent weeks, China has been accused of sponsoring a wave of denial-of-service attacks on GitHub, in an apparent effort to shut down portions of the site that host tools for getting around Chinese internet censorship.

In response to Obama's new executive order, a spokesperson for the Chinese government indicated that China is opposed - saying international cooperation "based on mutual respect and trust" is necessary to combat cyber threats.

When it comes to prosecuting attackers from nations like China and Russia, US law enforcement is severely limited.

The US hopes the new sanctions regime will be a deterrent against future attacks.

Lisa Monaco, a prosecutor in the US Department of Homeland Security, said the sanctions "increase the costs and reduce the economic benefit from malicious cyber activity."

The White House assured that the executive order "in no way" targets victims of cyberattacks - such as those whose computers have been exploited to launch attacks on others.

Some critics in the security community have argued that US computer security laws have a chilling affect on security research and could lead to prosecution of researchers.

The White House said the sanctions are not designed to "prevent or interfere with the cybersecurity research community" that identifies vulnerabilities in order to improve security of software and devices.

Cybercrime Fighting Group Takes Down Beebone Botnet

A new group of international cybercrime fighters claimed one of its first kills Thursday, pulling the plug on malicious servers that hijacked at least 12,000 machines, most of them in the United States.

The elimination of the Beebone botnet is an early success chalked up by the Joint Cybercrime Action Taskforce, a coordination body created last year by the FBI, Britain’s National Crime Agency, Europol and host of other international law enforcement agencies.

It’s also an illustration of the lengths many hackers go to defeat investigators. Beebone’s masters deployed shape-shifting software that updated itself up to 19 times a day.

"From a techie’s perspective, they made it as difficult as they possibly could for us," said Europol advisor Raj Samani, who spoke to The Associated Press on Wednesday, only an hour after authorities wrested the last rogue server from the criminals’ control.

Botnet is the term applied to networks of hijacked machines which criminals or security agencies use to spread malicious software, empty bank accounts and launch attacks.

Beebone was modest by botnet standards, but Samani the chief technology officer of Intel Security’s Europe, Middle East and Africa division said it was state-of-the-art. Beebone relied on a pair of malicious programs that re-downloaded each other, an insurance policy should one of them be removed. Regular tweaks to the software’s code made it difficult for experts to blacklist the programs.

"In terms of size this is obviously small, but in terms of sophistication, we’re talking about an investment by the criminals," he said.

The move is a big step for the Cybercrime Action Taskforce, set up in September in a bid to go after top-level Internet crime. A host of security groups including Intel Security, Kaspersky and Shadowserver provided assistance.

Europol would not name any of the victims of the botnet. Europol’s Paul Gillen said there had not yet been any arrests.

China Now Has an Internet Cannon. Wait, What’s an Internet Cannon?

On Friday morning, news reports surfaced that China had acquired an Internet cannon. And wait: What is this about China having an Internet cannon?

If you feel terrifyingly out of the loop, take a deep breath and read the following to learn more about what an Internet cannon is and what it can do.

What is an Internet cannon?

More commonly known in the hacker community as a Low Orbit Ion Cannon (LOIC or WebLOIC), an Internet cannon is a type of computer program used to force traffic overloads (or denial-of-service) onto targeted websites. It uses the Internet to blast out cyberattacks. It s not a literal cannon.

Why does China have one?

A new report and analysis claims that China is using what is being termed the Great Cannon, ostensibly a type of LOIC, to force an overflow of Web traffic and malicious code onto sites its government wishes to squash in the name of censorship. (If a website is overwhelmed by traffic, real or manufactured, no one will be able to visit it.) The new cybertool is being used in conjunction with its Great Firewall, which already blocks access to sites like Facebook and Twitter on Chinese networks.

Denial-of-service attacks on two GitHub project pages last month are now being credited to China s Great Cannon. The GitHub pages were hosting Chinese censorship circumvention projects run by the anonymous, presumably Chinese activist site GreatFire.org.

Jeesh. That sounds terrible. What kind of country would build such a heinous cyberweapon?

Well, the United States has a similar program.

According to the New York Times, information provided in the Edward Snowden leaks outlines U.S. government systems that can intercept and redirect Internet traffic to a site of their choosing.

Of course, we don t know of any instances where the U.S. has used an Internet cannon-type attack in domestic censorship.

 The N.S.A. and its partners appear to use the programs for targeted surveillance, whereas China appears to use the Great Cannon for an aggressive form of censorship, the Times piece explains.

Should the fact that China is using an Internet cannon scare me?

Though Friday s New York Times piece called the Great Cannon a powerful new weapon, developers are calling it OLD! They say the tool has been used by script kiddies and activists for the past four or so years.

Essentially any site is and has been vulnerable to attacks of this nature (though greater encryption can help better protect against them). So no one should be any more afraid of it happening today than ever before. The only difference now is that, if the Chinese government is found to be

attacking U.S.-hosted sites, we could have an international cyberdispute on our hands.

The last time we saw one of those, a very subpar movie made headlines all around the world and raked in an undeservingly large amount of money. A replay of something like that would be much scarier than your favorite website getting knocked offline for half a day.

Facebook Inc. Is Tracking Non-Users

Facebook Inc admitted that it s been tracking people who don t actually use its services. The company has long been suspected of such behaviour, given the wealth of knowledge it has access to through its social platforms, but has never admitted it before today.

According to the company a bug in its system caused people who had never agreed to the Facebook Inc terms and conditions to be tracked by the company s web software. The Menlo Park, California company denies that its breaches European privacy laws in the process of tracking those users. The information about the unseemly following emerged as part of a court case that the company is defending against in Austria.

Users may be familiar with the idea of being followed on a social network, but most would disagree with a world where social networks were tracking non users as they made their way across the web.

Richard Allan, the company s vice president for policy in Europe said The researchers did find a bug that may have sent cookies to some people when they weren t on Facebook. This was not our intention a fix for this is already under way.

According to the executive, Facebook does receive standard web impressions , or website visit information, when people visit sites with our plugins or other integrations. The authors misleadingly call this tracking. The social networks splitting of tracking from gathering impressions of web users is an interesting one, and questions like that will eventually sit at the heart of the current case.

Despite what a European court may think about the way Facebook Inc deals with user data, the company s investors aren t going to change their mind by many deviations. Since the beginning of the year shares in Facebook Inc have risen by more than 5%. The company s potential in the social marketing sector is palpable, and investors are betting big on the company.

Since the beginning of the year, many parts of Facebook s longer term strategy have become clear. The company is betting on its operation of a group of popular social networking applications to gather data for it, and drive revenues upward.

Facebook Hits Back at Report Claiming It Tracks Pretty Much Everyone

Facebook has hit back at a new report commissioned by the Belgian Privacy Commission, which claims that Facebook tracks far more users than

previously thought.

The report, conducted by researchers at universities in Leuven and Brussels, says the social giant is tracking the browsing habits of everyone visiting its site, irrespective of whether or not they are an account holder, and in complete disregard of whether or not they have opted out of being tracked across the EU.

Additionally, the report says Facebook also continues to track users after they close their accounts and sets tracking cookies on some third party websites. The researchers note that social plugins, such as the Like button, are often behind the setting of these third-party cookies, even if the user does not directly interact with them.

The researchers also say Facebook is placing tracking cookies every time a user visits tertiary pages on its site, such as celebrity pages or shops, all for the purpose of delivering targeted advertising based on other pages they visit across the internet.

Under EU law, websites must generally obtain consent before using a cookie and websites must seek permission from new users before placing them.

In theory, users who have previously consented to particular cookies, can later opt out of having their web browsing history tracked in this way by clicking an ad choices button or similar, as found on many different flavours of advertisements across the web. Taking this option typically allows the user to then choose which internet companies can and cannot track them, or even block them completely.

In the case of Facebook, however, the researchers say that an ’opt out’ request is interpreted in an unexpected way - it actually places an additional cookie on the user’s device.

That cookie - called ’datr’ - actually allocates a unique tracking number to the user’s device, allowing Facebook to track it for the next two years, as explained by one of the report’s authors, Günes Acar:

If people who are not being tracked by Facebook use the opt out mechanism proposed for the EU, Facebook places a long-term, uniquely identifying cookie, which can be used to track them for the next two years. What s more, we found that Facebook does not place any long-term identifying cookie on the opt-out sites suggested by Facebook for US and Canadian users.

Co-author Brendan Van Alsenoy told the Guardian how this policy contradicts existing law within the European Union:

European legislation is really quite clear on this point. To be legally valid, an individual’s consent towards online behavioural advertising must be opt-in.

Another of the co-authors, Rob Heyman, noted the irony brought about by Facebook’s cookie policy, saying:

If you take measures to protect your privacy from Facebook, you are actually going to be followed more on the internet.

Naturally, though, Facebook sees things differently to the report authors.

According to the Guardian, Facebook described the report as "inaccurate," and said there had been no contact between itself and the authors prior to publication.

A Facebook spokesperson told the news agency that the report was based on assumptions, and no clarification or comment had been sought before it was made public.

Facebook said it remained "willing to engage with them and hope they will be prepared to update their work in due course," adding:

Earlier this year we updated our terms and policies to make them more clear and concise, to reflect new product features and to highlight how we re expanding people s control over advertising. We re confident the updates comply with applicable laws including EU law.

The Dublin headquartered company also told the BBC that it had passed two audits of its data protection policies and that it continues to be regulated by the Irish Data Commissioner.

These new reports come just a few days after we brought you the news that European Commission attorney Bernhard Schima admitted that the EU-US Safe Harbor agreement, designed to protect the privacy of European citizens, was not working as intended.

His advice to privacy-conscious Facebook users: "consider closing your account".

Schima’s comment came not long after German privacy regulator Johannes Caspar, questioned Facebook’s new privacy policy - which some campaigners have suggested is just a rehash of the old one - and whether it breached the nation’s laws.

The social giant has other concerns too - Max Schrems and his ’Europe v Facebook’ group are not only challenging the Safe Harbor agreement in the European Court of Justice, but also seeking compensation for breach of privacy via a Vienna court too.

Schrems began that action last June, claiming that Facebook supplied personal information to the US Prism spy program. He, and the first 25,000 people who signed up to his group, have submitted a class action claim which seeks £400 compensation for each member. The court will decide whether the claimants can continue their action on 9 April.

If you’re concerned about tracking, try using a plugin for controlling which cookies you accept, such as Ghostery.

Google Clamps Down on Ad Injectors After 100,000 Chrome Users Complained

Google has picked a fight with ad injectors - programs that insert adverts into the pages you visit while browsing the web - following complaints from more than 100,000 of its Chrome users.

The search giant accumulated the huge pile of grumbles in just three months, demonstrating how users viewed the annoying and sometimes dangerous, browser-based ad injectors as a major gripe, surpassing

concerns over performance issues and network errors.

Writing for Google’s online security blog, software engineer Nav Jagpal said ad injectors are "part of an environment where bad practices hurt users, advertisers, and publishers alike," adding that:

People don t like ad injectors for several reasons: not only are they intrusive, but people are often tricked into installing ad injectors in the first place, via deceptive advertising, or software "bundles".

Jagpal was keen to point out that the blame for ad injectors should not lie solely with advertisers - many, he said, were unaware that their adverts were being injected at all and so had no idea where some of their ads were running.

Publishers are also victims in some senses he said, pointing out how they were not being compensated for displaying injected ads, and may be completely unaware that visitors to their sites were being put at risk by spam or injected malware.

So what is Google going to do about this menace?

Jagpal says the company already had policies in place that limited or prohibited ad injectors but, to further understand the issues, it commissioned a survey from the University of California, Berkeley.

The study crawled through data obtained from over 100 million page views of Google sites, using the Chrome, Firefox and Internet Explorer browsers.

The survey’s full findings will be made public on 1 May as part of an awareness program about ad injectors but, in the meantime, Google said of the data that came back: "It’s not a pretty picture".

The study, which was conducted on machines running both Windows and OS X, found ad injectors on both operating systems and in each of the three tested browsers.

Around 1 in 20 people visiting Google sites had at least one ad injector installed. Of those, half of the sample had a minimum of two injectors installed and nearly a third had four or more.

34% of Chrome extensions injecting ads were classified as outright malware.

The researchers also discovered 192 "deceptive" Chrome extensions affecting 14 million users, all of which have since been disabled.

Google says it has implemented techniques used in the research to better enable it to scan all new extensions, as well as old ones which get updated.

Commenting on the findings, Jagpal said:

We’re constantly working to improve our product policies to protect people online. We encourage others to do the same. We’re committed to continuing to improve this experience for Google and the Web as a whole.

That’s not to say Google will completely ban ad injectors though - it says users should have the freedom to install them if they wish - but the injectors must be completely transparent about what they do and not

overlay website ad space without permission from the site’s owner.

However, sneaky injectors that are designed to slip ads, or worse, into a user’s browser will not be welcome and Google says such software will definitely find itself in unwanted software policy territory.

To help users avoid installing rogue ad injectors in the future, Google will deploy its familiar red warning notice which will advise Chrome users that the web page is attempting to install ad-injecting software without having the correct browser APIs in place.

Apple Releases New OS X and iOS Updates

Apple is having a big Wednesday.

The morning saw the Internet abuzz over journalist reviews of the new Apple Watch. But then Apple announced big software updates to the operating systems for both its Mac line and iOS devices.

The version bumps (OS X 10.10.3 and iOS 8.3) bring the new iPhoto-replacing Photos app to Mac, and the new multi-ethnic emojis for iMessage to all of its mobile devices and computers.

The Photos app for OS X brings Mac laptops and desktops picture editing and cloud storing software that falls more in line with the look and feel of Apple s latest iOS apps. You can check out our David Pogue s hands-on impressions of the new Photos app right here.

There are also plenty of other tweaks and small additions in the iOS software upgrade, including more languages for Siri, and Wi-Fi and third-party keyboard fixes.

Apple made beta versions of these latest OS X and iOS releases available to the public a number of months ago, but Wednesday s releases will send the finished versions of the updates to all Mac, iPhone, iPad, and iPod touch owners.

These updates, in usual Apple fashion, should pop up on your device s screens and ask you you to install them. But if you re feeling impatient, you can see about getting them faster by going to the App Store on your Mac, and the General section under the Settings app on your iPhone or iPad.

Migrate Your Mac to OS X Yosemite 10.10.3 Immediately

Swedish hacker Emil Kvarnhammar is reporting that an unpublished OS X API he dubs it a "backdoor" can be used by nefarious types to gain root access through local users without Administrator status on Mac computers that have not yet been migrated to the 10.10.3 iteration of OS X, which was released just two days ago.

"The admin framework in Apple OS X contains a hidden backdoor API to root privileges [that] can be exploited to escalate privileges to root from any user account in the system," Kvarnhammar says in an advisory. "The

intention was probably to serve the System Preferences app and systemsetup command-line tool, but any user process can use the same functionality. This is a local privilege escalation to root, which can be used locally or combined with remote code execution exploits."

The OS X vulnerability that Kvarnhammar has dubbed Rootpipe was uncovered by the hacker last October, and it has taken Apple up until their recent security update to issue a patch for it. Unfortunately, however, only users who have installed Yosemite and who have updated their install to 10.10.3 will receive the patch. Specifically, what this means is that anyone driving a Mac running Mavericks, Mountain Lion, Lion, or Snow Leopard is potentially at risk of a security breach. Systems that are unable to migrate to Yosemite are out of luck.

At this point Rootpipe is a proof-of-concept developed by Kvarnhammar, and there have been no accounts of the vulnerability being leveraged in the wild. Kvarnhammar has published exploit code ahead of a talk he will give on May 28 at Security Conference in Stockholm next month, though, and enough information will be available following that event to allow smartie transgressors galore to put together their own versions of Rootpipe.

Though Yosemite is a free upgrade for anyone with a Mac capable of running the operating system (most iMacs and MacBook variations dating from mid-2007 or later), it is known to slow down some older systems and for that reason many owners of such systems have opted not to upgrade. In the face of a vulnerability such as Rootpipe and its cousins sure to come, however, these users as well as users of more recent systems who have decided to stick with earlier iterations of OS X will want to make the move to Yosemite. And fast.

Facebook Still Cool Among Teens, Says Survey

Facebook is still a "dominant force’ among teens, says a new survey. CNET Facebook remains the most popular social network among teens ages 13 to 17, according to a new Pew survey.

Though such sites as Instagram and Snapchat increasingly appeal to teens, Facebook is still a "dominant force," Pew said Thursday. Among the more than 1,000 teens surveyed, 71 percent said they use Facebook, while 41 percent said Facebook is the site they use the most frequently over all other social networks. Instagram and Snapchat scored as the second and third most frequently used sites, respectively.

Retaining and even building the teenage audience is critical to Facebook to attract advertising dollars, both in the present and especially in the future. Meanwhile, Facebook’s role in the life of the typical teen has been repeatedly called into question in recent years.

Surveys released last year, such as those from Piper Jaffray and Frank N. Magid Associates, have concluded that Facebook’s popularity among teenagers has dropped over the last few years. However, a Forrester poll last year was more in line with the new Pew survey and noted that Facebook is still the most frequently-used social media site among teens.

In October 2013, Facebook Chief Financial Officer David Ebersman said that daily Facebook use among younger teens had declined from the second quarter to the third quarter. But the next month, Facebook Chief

Operating Office Sheryl Sandberg dismissed such concerns, saying that "the vast majority of US teens are on Facebook, and the majority of US teens use Facebook almost every day."

According to the new Pew survey, most teenagers spend their time on more than one social network. But among the 22 percent who still use only one site, 66 percent pick Facebook, 13 percent use Google+, 13 percent Instagram and 3 percent Snapchat.

Boys were more likely than girls to say they visit Facebook most often (45 percent of boys versus 36 percent of girls). Girls polled were more likely than boys to say the same of Instagram and Tumblr.

Older teens from 15 to 17 years old were more likely than younger teens ages 13 to 14 to point to Facebook as their most used site (44 percent of older teens versus 35 percent of younger teens). Younger teens were more keen on Instagram than were older teens. That's still good news for Facebook since the company paid $1 billion to acquire Instagram in 2012.

Pew also questioned teens about their number of Facebook friends. Among those polled, the typical teenager has 145 friends on the network. Breaking it down, 30 percent reported somewhere between 0 and 100 friends, 12 percent between 101 and 200 friends, 9 percent between 201 and 300 and 15 percent more than 300. Around a third of the teens surveyed said they weren't sure how many Facebook friends they have.

Pew's survey was conducted online in the US in English and Spanish among about 1,060 teens ages 13 to 17 along with a parent or guardian from September 25 to October 9, 2014 and to 44 more teen/parent pairs from February 10 to March 16, 2015.

Facebook did not immediately respond to CNET's request for comment.

Internet Naming Group Asks FTC To Investigate .sucks Controversy

The group that oversees the Internet's naming and address system on Thursday asked the Federal Trade Commission to review whether any laws have been broken in the roll out of a new .sucks domain.

Currently, only trademark holders and celebrities may register Internet addresses ending in .sucks at a cost of more than $2,000 per name. Once the early registration period ends, ordinary people will be able to register .sucks names for as little as $10 in June.

The Internet Corporation for Assigned Names and Numbers (ICANN), a non-profit that sets policies for the global domain name system, said in a letter to the FTC and Canada's Office of Consumer Affairs that companies have complained the system is "predatory, exploitive and coercive."

ICANN asked the regulatory bodies to determine whether any laws had been broken. "ICANN is concerned about the contentions of illicit actions being expressed, but notes that ICANN has limited expertise or authority to determine the legality of Vox Populi's positions, which we believe would fall in your respective regulatory regimes," the group said in the letter.

Vox Populi Registry Inc, a Canadian firm, was awarded a contract last year to run the .sucks domain and established the pricing policy. "I don't think that anyone who takes a look will find a problem," Vox CEO John Berard said. "After all, the VoxPop sunrise price is well below the highest cost charged by at least one other registry and the price itself is somewhat misunderstood; most .sucks registrations seem to be taking place at $2,024."

Big companies and celebrities have been up in arms about the rollout of new Internet address names ending in .sucks since the idea first surfaced. But despite the protests, top companies such as Apple, Microsoft and Home Depot along with celebrities like Taylor Swift and Oprah Winfrey have been registering .sucks domains in the pre-registration period.

The moves, though spendy, prevent anyone else from controlling the website names when public registration for .sucks names opens in June. Consumer advocates supported the new domain name space as an opportunity for people to voice their complaints about businesses and, they hoped, get quicker responses.??The new .sucks Internet address is one of the most controversial among hundreds of new suffixes approved by ICANN. The group established a procedure for adding new suffixes in 2011 and has been slowly working its way through almost 2,000 initial applications. So far, it has approved almost 600, with new additions released daily.??The new suffixes are intended to unleash a barrage of creative energy, and perhaps a few marketing dollars, by breaking free of the crowded .com space. Over 100 million names have already been taken in .com, including almost every word in the dictionary. Most of the new additions are uncontroversial and inoffensive, such as .cafe, .gold and .tennis.??Vox Populi charges Internet registrars a wholesale price of $2,000 for .sucks names during the early preregistration period, with a recommended retail price of $2,500. Once general registration opens, the .sucks names will cost $250 for consumers. There's also a limited $10-a-year option if a consumer agrees to make the site part of Vox Populi's discussion network.

=~=~=~=

Atari Online News, Etc. is a weekly publication covering the entire Atari community. Reprint permission is granted, unless otherwise noted at the beginning of any article, to Atari user groups and not for profit publications only under the following terms: articles must remain unedited and include the issue number and author at the top of each article reprinted. Other reprints granted upon approval of request. Send requests to: dpj@atarinews.org

No issue of Atari Online News, Etc. may be included on any commercial media, nor uploaded or transmitted to any commercial online service or internet site, in whole or in part, by any agent or means, without the expressed consent or permission from the Publisher or Editor of Atari Online News, Etc.

Opinions presented herein are those of the individual authors and do not necessarily reflect those of the staff, or of the publishers. All material herein is believed to be accurate at the time of publishing.